DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE

SUBJECT **MICROCOMPUTER DATA STORAGE AND BACK-UP**	POLICY NO. **302.10**	EFFECTIVE DATE **10/1/89**	PAGE **1 of 3**
APPROVED BY: **Original signed by:** **ROBERTO QUIROZ** Director	SUPERSEDES **103.2 7/13/89**	ORIGINAL ISSUE DATE **7/13/89**	DISTRIBUTION LEVEL(S) **1**

PURPOSE

1.1   To ensure that all system files are backed-up and retained for an adequate period of time for reconstructive purposes in the event of accidental or deliberate loss of data.

POLICY

2.1   It shall be the responsibility of the Bureau Director, District/Division Chief, or Program Head or designee to implement, monitor, and enforce this policy and procedure.

2.2   All back-up media equipment within the Department of Mental Health (DMH) shall be compatible.

2.3   All hard disk work stations with a capacity of forty (40) megabytes or greater shall be fitted to receive data storage back-up equipment.

2.4   Audit trails shall include the identification of the individual who performed the transaction and shall be retained for a reasonable period of time.

2.5   All DMH microcomputer users shall be aware of the procedures stated below.

PROCEDURE

3.1   Back-up (copy) all system data periodically on disks or tape and store in a place secure from damage or theft. Determine how long data will be retained for reconstructive purposes in the event of accidental or deliberate loss of data.

3.2   Ensure against accidental loss of data by following these guidelines:

    3.2.1   Always store disks in protective sleeves, away from dust, smoke, and liquids.

    3.2.2   Do not touch the exposed surface of the disk or insert any foreign object into the disk drive of the computer.

    3.2.3   Be extremely cautious when formatting a disk. If unfamiliar with this procedure, ask for assistance.

DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE

SUBJECT: **MICROCOMPUTER DATA STORAGE AND BACK-UP**	POLICY NO. **302.10**	EFFECTIVE DATE **10/0/89**	PAGE **2 of 3**

3.2.4   Do not eat, drink, or smoke near the microcomputer and/or where data is stored.

3.2.5   Do not place disks or tapes near magnetic sources, e.g., telephones, radio speakers, or paper clips.

3.2.6   Do not label disks with either ball point or hard tipped pens; use felt tip pens.

3.2.7   Do not bend or place objects on top of disks.

3.3   Ensure the accuracy and reliability of the data and output, and identify the individual who performed the task by following these guidelines:

3.3.1   Retain source documents to permit tracing of the task to or from output reports or files.

3.3.2   Have sufficient information contained on output reports or files to enable the tracing of the work to its source documents.

3.3.3   List and maintain all work files stored on either floppy disk or the hard disk.

3.3.4   Maintain a report calendar sheet listing all output reports produced by the system to assure that all required reports are produced.

3.3.5   Review data, e.g., spreadsheets, data bases, documents, and output reports for completeness and scan for obvious errors prior to distribution.

3.3.6   Maintain adequate distribution instructions for all reports, including a listing of individuals who are to receive the report.

3.4   Include the following information, when appropriate, on each page of output reports:

3.4.1   Title of the report

3.4.2   Date

3.4.3   Report period covered

3.4.4   Report number (if applicable)

3.4.5   Page number

DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE

SUBJECT: **MICROCOMPUTER DATA STORAGE AND BACK-UP**	POLICY NO. **302.10**	EFFECTIVE DATE **10/0/89**	PAGE **3 of 3**

3.4.6 Sensitive or confidential data should, on each page, be clearly marked as "Confidential" or "Classified" and if appropriate, print classification and if distribution should be restricted accordingly.

3.4.7 An identification of the individual(s) who produced the report, the bureau, division, etc., and where the file is located, e.g., disk number or subdirectory.

AUTHORITY

County Fiscal Manual, Section 12.1.3
Auditor Controller ICCP Audit, 1988